WHAT IS CLAIMED IS:

1. A data control method comprising the steps of:

A) at least one of the following steps:

A-1) embedding prohibition information in data, wherein copying of the data is to be prohibited; and

A-2) embedding the prohibition information and N pieces of permission information in the data (N is a natural number), wherein the copying of the data is to be permitted N times; and

B) detecting the prohibition and/or permission information prior to the copying of the data,

wherein in the case where the permission information is detected from the data prior to the copying of the data, at least one of the N pieces of permission information in the data is invalidated, and then the copying of the data is permitted, and wherein in the case where the permission information is not detected from the data, and the prohibition information is detected from the data prior to the copying of the data, the copying of the data is prohibited.

2. A data control method according to claim 1, wherein the permission information is a digital signature f(M); and the digital signature f(M) is derived based on a digital code M which is extracted from the data.

3. A method for embedding data control information comprising one of the following steps:

embedding prohibition information in data, wherein copying of the data is to be prohibited; and

embedding the prohibition information and N pieces of permission information in the data (N is a

natural number), wherein the copying of the data is to be permitted N times.

4. A method for embedding data control information according to claim 3, wherein the permission information is a digital signature f(M) for a digital code M which is uniquely derived from the data.

5. A method for detecting data control information comprising the step of:

detecting predetermined permission and/or prohibition information prior to copying of data,

wherein in the case where the predetermined permission information is detected from the data prior to the copying of the data, the predetermined permission information is invalidated, and then the copying of the data is permitted, and wherein in the case where the predetermined permission information is not detected from the data, and the predetermined prohibition information is detected from the data prior to the copying of the data, the copying of the data is prohibited.

6. A method for detecting data control information comprising the step of:

authenticating a digital signature f(M) in data based on a digital code M which is derived from data,

wherein in the case where the digital signature f(M) in the data is authenticated prior to copying of the data, the copying of the data is permitted, and wherein in the case where the digital signature f(M) in the data is not authenticated prior to the copying of the data, the copying of the data is prohibited.

7. A device for embedding data control information, comprising:

a section for embedding prohibition information, which embeds prohibition information indicating at least a prohibition against copying of data in the data; and

a section for embedding permission information, which embeds N pieces of permission information in the data along with the embedding of the prohibition information by the section for embedding prohibition information in the case where the copying of the data is to be permitted N times, wherein N is a natural number.

8. A device for embedding data control information according to claim 7, wherein the section for embedding permission information has a code extracting section for extracting a digital code M from the data.

9. A device for embedding data control information according to claim 8, wherein the section for embedding permission information includes: a signature section for generating a digital signature f(M) based on the digital code M which is extracted by the code extracting section and a first public key held by a producer of the data; and a signature embedding section for embedding the digital signature f(M) generated by the signature section in the data as the permission information.

10. A device for detecting data control information which extracts prohibition information and permission information embedded in data, comprising:

a permission information detecting section for detecting the permission information from the data;

a permission information invalidating section for

invalidating the permission information in the data;

a prohibition information detecting section for detecting the prohibition information from the data; and

a determining section which sets a copy permission/prohibition flag to be in a copy permissive state and then outputs the flag in the case where the permission information is detected by the permission information detecting section; and sets the copy permission/prohibition flag to be in a copy prohibited state and then outputs the flag in the case where the permission information is not detected by the permission information detecting section, and the prohibition information is detected by the prohibition information detecting section.

11. A device for detecting data control information according to claim 10, wherein the permission information detecting section has a code extracting section for extracting a digital code M from the data.

12. A device for detecting data control information according to claim 11, wherein the permission information detecting section includes: a signature extracting section for extracting a digital signature f(M) which is embedded in the data; and an authentication section which generates a digital signature f(M) based on the digital code M extracted by the code extracting section and a second public key, compares the generated digital signature f(M) with the digital signature f(M) extracted by the signature extracting section, and validates a copy permission flag and outputs the flag if the digital signature f(M) is authenticated.

13. A device for recording data on a recording medium, comprising:

a permission information detecting section for detecting the permission information from the data;

a permission information invalidating section for invalidating the permission information in the data;

a prohibition information detecting section for detecting the prohibition information from the data; and

a determining section which sets a copy permission/prohibition flag to be in a copy permissive state and then outputs the flag in the case where the permission information is detected by the permission information detecting section; and sets the copy permission/prohibition flag to be in a copy prohibited state and then outputs the flag in the case where the permission information is not detected by the permission information detecting section, and the prohibition information is detected by the prohibition information detecting section; and

a data recording section which records the data in the case where the copy permission/prohibition flag is set to be in the copy permissive state by the determining section, and does not record the data in the case where the copy permission/prohibition flag is set to be in the copy prohibited state by the determining section.

14. A device for recording data according to claim 13, wherein the permission information detecting section has a code extracting section for extracting a digital code M from the data.

15. A data control method comprising the steps of:

A) at least one of the following steps:

A-1) embedding prohibition information in data, wherein processing of the data is to be prohibited; and

A-2) embedding the prohibition information and N pieces of permission information in the data (N is a natural number), wherein the processing of the data is to be permitted N times; and

B) detecting the permission and/or prohibition information prior to the processing of the data,

wherein in the case where the permission information is detected from the data prior to the processing of the data, at least one of the N pieces of permission information in the data is invalidated, and then the processing of the data is permitted, and wherein in the case where the permission information is not detected from the data, and the prohibition information is detected prior to the processing of the data, the processing of the data is prohibited.

16. A method for embedding data control information comprising one of the following steps of:

embedding prohibition information in data, wherein processing of the data is to be prohibited; and

embedding the prohibition information and N pieces of permission information in the data (N is a natural number), wherein the processing of the data is to be permitted N times.

17. A method for detecting data control information comprising the following step of:

detecting predetermined permission and/or prohibition information prior to processing of data,

wherein in the case where the predetermined permission information is detected from the data prior to the

processing of the data, the predetermined permission information is invalidated so as to permit the processing of the data, and wherein in the case where the predetermined permission information is not detected from the data, and the predetermined prohibition information is detected from the data prior to the processing of the data, the processing of the data is prohibited.

18. A device for embedding data control information, comprising:

a section for embedding prohibition information, which embeds prohibition information indicating prohibition against processing of data in the data; and

a section for embedding permission information, which embeds N pieces of permission information in the data along with the embedding of the prohibition information by the section for embedding prohibition information in the case where the processing of the data is to be permitted N times, wherein N is a natural number.

19. A device for detecting data control information which extracts prohibition information and permission information embedded in data, comprising:

a permission information detecting and deleting section which, in the case where N pieces of permission information (N is a natural number) are detected from the data, invalidates at least one of the N pieces of permission information in the data, validates a permission flag, and outputs the flag;

a prohibition information detecting section which validates a prohibition flag and outputs the flag in the case where the prohibition information is detected from

the data; and

a determining section which sets a permission/prohibition flag to be in a permissive state and then outputs the flag when the permission flag is valid or the prohibition flag is not valid, and sets the permission/prohibition flag to be in a prohibited state and then outputs the flag when the permission flag is invalid and the prohibition information is valid.